REMARKS

I. General

Claims 1-23 were pending in the present application. The current Office Action (mailed March 23, 2006) rejects all claims 1-23. The outstanding issues raised in the current Office Action are:

- Claims 1-3, 6-9, 11, 14-16, 18, and 21-23 are rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,347,374 issued to Drake et al. (hereinafter "*Drake*"); and

- Claims 4-5, 10, 12-13, 17, and 19-20 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Drake* in view of U.S. Patent No. 6,775,657 issued to Baker (hereinafter "*Baker*").

Applicant respectfully traverses the outstanding claim rejections raised in the current Office Action, and requests reconsideration and withdrawal thereof in light of the amendments and remarks presented herein.

II. Amendments

Independent claims 1, 9, and 16 are amended herein. Support for the amendments can be found, *inter alia*, at page 9, line 25 – page line, line 14 of the specification. Thus, no new matter is added by these amendments.

III. Rejections Under 35 U.S.C. §102 over *Drake*

Claims 1-3, 6-9, 11, 14-16, 18, and 21-23 are rejected under 35 U.S.C. § 102(e) as being anticipated by *Drake*. To anticipate a claim under 35 U.S.C. § 102, a single reference must teach every element of the claim, *see* M.P.E.P. § 2131. Applicant submits that claims 1-3, 6-9, 11, 14-16, 18, and 21-23 are not anticipated by *Drake* because *Drake* fails to teach each and every element of these claims, as discussed below.

Independent Claim 1

Independent claim 1, as amended herein, recites:

> A method of presenting data related to an intrusion event on a computer system, comprising:
> capturing data related to the intrusion event;
> decoding the captured data from a predetermined format to a predetermined format decipherable by humans, the decoded data in turn comprises intrusion event data, data summary, and detailed data;
> presenting the decoded data to a user in an organized manner;
> determining at least one data component of the presented decoded data that is related to another data component of the presented decoded data; and
> graphically identifying the at least one data component of the presented decoded data. (Emphasis added).

Drake fails to teach each and every element above. First, *Drake* fails to teach determining at least one data component of presented decoded that is related to another data component of the presented decoded data. *Drake* provides no teaching of determining any presented data components that are related to another data component of the presented decoded data. Further, *Drake* provides no teaching of graphically identifying the determined related data component(s). The present application teaches, at page 9, line 25 – page line, line 14, determining related data components of the presented decoded data and graphically identifying (e.g., highlighting) such data components that are related is very useful in assisting the user in decoding and/or understanding the information being presented. *Drake*, on the other hand, simply provides no teaching whatsoever of providing such a feature. Further, the above elements of claim 1 are not taught or suggested by any other reference applied by the Examiner.

In view of the above, the rejection of claim 1 should be withdrawn.

Independent Claim 9

Independent claim 9, as amended herein, recites:

> A method of presenting data of an intrusion detection system, comprising:
> capturing, from a network, data related to an intrusion event in response to a trigger;
> decoding the captured data from a first predetermined format to a second predetermined format, the decoded data comprising network header data, data summary, and detailed data;
> presenting the decoded data according to a predetermined report format;
> receiving user input graphically highlighting a first data component of the presented decoded data;
> determining at least one other data component of the presented decoded data that is related to the first data component; and
> graphically highlighting the at least one other data component of the presented decoded data. (Emphasis added).

Drake fails to teach each and every element above. First, as discussed above with claim 1, *Drake* fails to teach determining at least one data component of presented decoded that that is related to a user-selected data component of the presented decoded data. *Drake* provides no teaching of receiving user input graphically highlighting a first data component of the presented decoded data, and further provides no teaching of determining any other presented data components that are related to the user-highlighted data component. Further, *Drake* provides no teaching of graphically highlighting the determined related data component(s). The present application teaches, at page 9, line 25 – page line, line 14, that enabling a user to select one of the presented data components and have the user interface, in response to such selection, graphically highlight the other presented data components that are related to the user-selected data component is very useful in assisting the user in decoding and/or understanding the information being presented. *Drake*, on the other hand, simply provides no teaching whatsoever of providing such a feature. Further, the above elements of claim 9 are not taught or suggested by any other reference applied by the Examiner.

In view of the above, the rejection of claim 9 should be withdrawn.

Independent Claim 16

Independent claim 16, as amended herein, recites:

> A system of presenting data of an intrusion detection system, comprising:
> a network driver capturing data related to an intrusion event from a network;
> a decode engine decoding the captured data from a predetermined format to a predetermined format decipherable by humans, the decoded data comprising intrusion event data, data summary, and detailed data;
> a mapping table that correlates related data components of the decoded intrusion event data, data summary and detailed data; and
> a user interface presenting the decoded data to a user, wherein the user interface is operable, responsive to receiving user input selecting a first data component of one of the presented decoded intrusion event data, data summary and detailed data, to graphically identify any data components of the others of the presented decoded intrusion event data, data summary and detailed data that the mapping table correlates to the first data component. (Emphasis added).

Drake fails to teach each and every element above. First, *Drake* fails to teach a user interface that receives user input selecting a first data component of one of the presented decoded intrusion event data, data summary, and detailed data. Further, *Drake* fails to teach graphically identifying any data components of the others of the presented decoded intrusion event data, data summary and detailed data that a mapping table correlates to the user-selected data component. In other words, *Drake* fails to teach a user interface that enables a user to select a data component in one of the presented decoded intrusion event data, data summary, and detailed data; and then graphically identifies any correlated data components in the others of the presented decoded intrusion event data, data summary, and detailed data.

The present application teaches, at page 9, line 25 – page line, line 14, that enabling a user to select one of the presented data components and have the user interface, in response to such selection, graphically identify (e.g., highlight) the other presented data components that are related to the user-selected data component is very useful in assisting the user in decoding and/or understanding the information being presented. For instance, by selecting a data element in one of the presented decoded intrusion event data, data summary, and detailed data, the user interface graphically identifies the correlated data components in the other ones of the presented decoded intrusion event data, data summary, and detailed data. This aids a

user in understanding the correlated data components in the various portions of the presented data. *Drake*, on the other hand, simply provides no teaching whatsoever of providing such a feature. Further, the above elements of claim 16 are not taught or suggested by any other reference applied by the Examiner.

In view of the above, the rejection of claim 16 should be withdrawn.

Dependent Claims 2-3, 6-8, 11, 14-15, 18, and 21-23

Claims 2-3, 6-8, 11, 14-15, 18, and 21-23 each depend either directly or indirectly from one of independent claims 1, 9, and 16, and thus inherit all limitations of the respective independent claim from which they depend. It is respectfully submitted that dependent claims 2-3, 6-8, 11, 14-15, 18, and 21-23 are allowable not only because of their dependency from their respective independent claim for the reasons discussed above, but also in view of their novel claim features (which both narrow the scope of the particular claims and compel a broader interpretation of the respective independent claim from which they depend).

IV. Rejections Under 35 U.S.C. §103 over *Drake* in view of *Baker*

Claims 4-5, 10, 12-13, 17, and 19-20 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Drake* in view of *Baker*. Claims 4-5, 10, 12-13, 17, and 19-20 each depend either directly or indirectly from one of independent claims 1, 9, and 16, and thus inherit all limitations of the respective independent claim from which they depend. As discussed above, claims 1, 9, and 16 are believed to be of patentable merit over *Drake*. Further, *Baker* does not resolve the above-identified deficiencies of *Drake* with regard to claims 1, 9, and 16. Applicant therefore respectfully submits that dependent claims 4-5, 10, 12-13, 17, and 19-20 are allowable not only because of their dependency from their respective independent claim for the reasons discussed above, but also in view of their novel claim features (which both narrow the scope of the particular claims and compel a broader interpretation of the respective independent claim from which they depend).

V. Conclusion

In view of the above, Applicant believes the pending application is in condition for allowance.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 08-2025, under Order No. 10017330-1 from which the undersigned is authorized to draw.

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail, Label No. EV 568242777US in an envelope addressed to: M/S Amendment, Commissioner for Patents, Alexandria, VA 22313.

Date of Deposit: June 23, 2006

Typed Name: Gail L. Miller

Signature: Gail L. Miller

Respectfully submitted,

By: Jody C. Bishop

Jody C. Bishop
Attorney/Agent for Applicant(s)
Reg. No. 44,034
Date: June 23, 2006
Telephone No. (214) 855-8007